A SURVEY ON INNOVATIONS IN BLOCK CHAIN TECHNOLOGY

G.JayanthiLakshmi
Assistant Professor
Dept of CSE
ASCET, Gudur.

YL Saathvika
UG Student
Dept of CSE
ASCET, Gudur

PV KrishnaVamsi
UG Student,
Dept of CSE
ASCET, Gudur.

V Prathima
UG Student
Dept of CSE
ASCET, Gudur

ABSTRACT:

Block chain is as of late presented and changing the advanced world conveying another point of view to security, flexibility and productivity of framework. While at first promoted by Bit Coin, Block chain is significantly more than an establishment for digital money. It offers a safe method to trade any sort of good administration or exchange. This paper exhibits an exhaustive review on Block chain Technology. In this we talk about Block chain design, applications, specialized difficulties and late advances. We also format conceivable future patterns for Block chain.

Key words: Block chain, Bit coin, Internet of Things (IOT), E-Voting, Trade and Finance, supply chain.

I.INTRODUCTION

Blockchain: A Blockchain is a standout amongst the most famous and dubious syndicated programs among innovation pioneers. In basic words blockchain is a sort of computerized record, a record of exchanges without the control of any focal expert. Every one of the exchanges are put away as squares. Blockchain is the most recent method for putting away information and exchanges. At the end of the day, blockchain is a disseminated record guardian to store exchange information without focal man.

A blockchain is a chain of blocks of that develops as new information is added to the chain. Each "Block" contains a hashed key which joins it to the past block, a timestamp for when it was adjusted, and exchange information. Every exchange is confirmed by the minors and added to the block blockchain after accord is come to on the legitimacy of the activity. This enables members to put trust in their exchanges even without a focal specialist, along these lines empowering disint mediation.

A blockchain is intrinsically unchanging - when recorded, information on the blockchain can't be changed. In a blockchain to refresh an old record, most of the hubs must be consented to change. Blockchain innovation is one of the rising advancements now days. It might bring us more dependable and helpful Services. Blockchain is a group of innovations containing scientific calculation, Cryptography, shared systems, circulated database.

II LITERATURE SURVEY

Blockchain is a conveyed record innovation, ordinarily utilized in the digital money Bitcoin. The Financial Times (2016) characterizes Blockchain as a “network of computers, all of which must endorse an exchange has occurred before it is recorded, in a 'chain' of PC code. The subtle elements of the exchange are recorded on an open record that anybody on the system can see."

In 2008, Satoshi Nakamoto acquainted the world with Bitcoin by discharging the paper, "Bitcoin: A Peer-to-Peer Electronic Cash System."[1] The proposition was to circulate electronic exchanges instead of keep up reliance on unified foundations for the trade. When taking a gander at Bitcoin the new idea is the Blockchain structure dependent on research for time stepping bundles and ensuring the chain of care. Blockchain is basically an improved installment check framework. Bitcoin and by augmentation, Blockchain, are acknowledging consistent development. At the season of this paper, insights from Blockhain.info demonstrate a $15.3B showcase top and $314.7M in exchanges every day. Notwithstanding the development, numerous inquiries encompass broad reception of Bitcoin. Be that as it may, the fundamental structure has picked up consideration with application outside of the money related world.

Blockchain will develop in various zones as the assortment of research develops. Scientists are attempting to apply various utilize cases included savvy contracts, inventory network, and medicinal services [2] (PHI) as this paper illustrates. Relate Professor of Computer Science at Cornell Emin Gün Sirer, has watched, "The Internet of Things could be a huge application territory where individuals need to speak with gadgets, yet not through middle people. There is no executioner application yet, however it is probably going to include the straightforwardness of Blockchain [3]." Today, scientists are centered around security, protection, and versatility of Blockchain. In his April, 2016 piece, "May Blockchain Outlive Bitcoin?" Hurlburt tends to the requirement for morals and operational direction seeing before Blockchains turned out to be typical swap for conventional exchange databases, strict measures, including satisfactory conduct rules, must be lay out.

We began with a money related application for exchanges in Bitcoin. The roof is high and desires are vast for Blockchain. Applications change and numerous technologists are bullish on what's to come. For instance, advanced business visionary Blythe Masters specifies "you ought to consider this innovation [Blockchain] as important as you ought to have been taking the improvement of the Internet in the mid 1990's. It's closely resembling email for cash [4]." Michael Harte, CTO at Barclays recommends the transformative idea of Blockchain, "we could go the manner in which that record exchange innovation changed music, permitting new organizations like iTunes to develop [5]."

III.CHARACTERISTICS OF BLOCKCHAIN

Key Characteristics of Blockchain In summary, blockchain has following key characteristics.

• Decentralization. In traditional incorporated exchange frameworks, every exchange should be approved through the focal confided in organization (e.g., the national bank), unavoidably coming about to the expense and the execution bottlenecks at the focal servers. Complexity to the concentrated mode, outsider is never again required in blockchain. Accord calculations in Block Chain are utilized to keep up information consistency in disseminated organize.

• Persistency. Exchanges can be approved rapidly and invalid exchanges would not be conceded by legit diggers. It is about difficult to erase or rollback exchanges once they are incorporated into the Block Chain. Hinders that contain invalid exchanges could be found promptly.

• Anonymity. Every client can collaborate with the Block Chain with a produced location, which does not uncover the genuine character of the client. Note that Block Chain can't ensure the ideal security protection because of the inherent requirement.

• Auditability. Bitcoin Block Chain stores information about client adjusts dependent on the Unspent Transaction Output (UTXO) show: Any exchange needs to allude to some past unspent exchanges. When the present exchange is recorded into the Block Chain, the condition of those alluded unspent exchanges change from unspent to spent. So exchanges could be effectively verified and followed.

IV.APPLICATIONS OF BLOCKCHAIN

S.No	APPLICATION	DESCRIPTION
1	Block Chain in Real estate	In the real estate market there are various individual angles that are to be kept mystery to make a focused market. Blockchain innovation could empower the land advertise more straightforward and free from arbiter. Utilization of blockchain in land makes the work quicker, less demanding, riskless, lessening extortion and giving more straightforwardness. Blockchain as keen contracts can assume a major job in land, particularly in activities, for example, property exchanges (buy, deal, financing, renting, and administration).
2	Blockchain in Supply Chain	Traditional supply chains need straightforwardness in view of their multifaceted nature. Blockchain innovation is greatly affecting business to make straightforwardness. Presently days associations are tolerating advanced method for supply chains. New advances, having extraordinary effect in transit of business. These strategies are on a very basic level changing the manner in which things are delivered and disseminated. In store network blockchain is being acknowledged step by step.
3	Blockchain for e-voting	Innovation is getting advance step by step. Electronic casting a ballot framework is the most recent creation of this specialized world. Just in the couple of years e-casting a ballot framework turn out to be excessively famous due to its straightforwardness, high security and protection. Cryptography is utilized to make the framework more secure. In e-casting a ballot framework all capacities are on the web and result is tallied consequently. Contrasted and customary casting a ballot, electronic casting a ballot is less tedious and rate of exactness is more. Utilization of blockchain

		makes it more straightforward and secure.
4	Blockchain in Education	Blockchain is endeavor to have a place in every single field. The utilization of blockchain to instruction is somewhat new. Blockchain can be utilized to join the records of expansive colleges, little foundations, schools and online instructive stages to shape a freely obvious chain.
5	Blockchain in Medical	Blockchain innovation can likewise assume an essential job in medicinal services moreover. Blockchain has transformative potential for our wellbeing and care frameworks. There are various utilize instances of blockchain in medicinal services, for example, repayment of social insurance administrations, trade of wellbeing information, clinical preliminaries and supply chains. In spite of the fact that having an extraordinary effect in therapeutic, this innovation yet confronting various difficulties that are keeping the usage of this innovation in restorative, for example, information protection and clinical preliminaries.

V. CHALLENGES &RECENT ADVANCES

Despite the great potential of blockchain, it faces numerous challenges, which limit the wide usage of blockchain. We enumerate some major challenges and recent advances as follows.[9]

A. Scalability With the amount of transactions increasing day by day, the blockchain becomes bulky. Each node has to store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacityof blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee. There are a number of efforts proposed to address the scalability problem of blockchain, which could be categorized into two types:

- Storage optimization of blockchain.
- Redesigning blockchain.

B. Privacy Leakage

Blockchaincanpreserveacertainamountofprivacythrough the public key and private key. Users transact with their private key and public key without any real identity exposure. However, it is shown in [10], [11] that blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study [12] has shown that a user's Bitcoin transactions can be linked to reveal user's information. Moreover, Biryukov et al. [13] presented an method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In [13], each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve anonymity of blockchain, which could be roughly categorized into two types:

- Mixing
- Anonymous.

C. Selfish Mining

Blockchain is susceptible to attacks of colluding selfish miners. In particular, Eyal and Sirer [14] showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publishment, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Based on selfish mining, many other attacks have been proposed to show that blockchain is not so secure. In stubborn mining [15], miners could amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategy that miners still mine the blocks even if the private chain is left behind. Yet in some cases, it can result in 13% gains in comparison with a non-trail-stubborn counterpart. [16] shows that there are selfish mining strategies that earn more money and are profitable for smaller miners compared to simple selfish mining. But the gains are relatively small. Furthermore, it shows that attackers with less than 25% of the computational resources can still gain from selfish mining. To help fix the selfish mining problem, Heilman [17] presented an novel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners would select more fresh blocks. However, [17] is vulnerable to forgeable timestamps. ZeroBlock [18] builds on the simple scheme: Each block must be generated and accepted by the network within a maximum time interval. Within ZeroBlock, selfish miners cannot achieve more than its expected reward.

VI. POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its potential in industry and academia. We discuss possible future directions with respect to four areas: blockchain testing, stop the tendency to centralization, big data analytics and blockchain application.

A. Blockchain testing

As of late various types of blockchains show up and more than 700 digital currencies are recorded in [19] up to now. Be that as it may, a few engineers may adulterate their blockchain execution to draw in speculators driven by the immense profit. Other than that, when clients need to join blockchain into business, they need to know which blockchain fits their prerequisites. So blockchain testing system should be set up to test diverse blockchains. Blockchain testing could be isolated into two stages: institutionalization stage and testing stage. In institutionalization stage, all criteria must be made and concurred. At the point when a blockchain is conceived, it could be tried with the concurred criteria to legitimate if the blockchain works fine as designers guarantee. Concerning testing stage, blockchain testing should be performed with various criteria. For instance, a client who is accountable for online retail business thinks about the throughput of the blockchain, so the examination needs to test the normal time from a client send an exchange to the exchange is stuffed into the blockchain, limit with respect to a blockchain square and so on.

B. Stop the tendency to centralization

Blockchain is structured as a decentralized framework. Notwithstanding, there is a pattern that mineworkers are concentrated in the mining pool. Up to now, the best 5 mining pools together possesses bigger than 51% of the aggregate hash control in the Bitcoin organize [20]. Aside from that, selfish mining methodology [21] demonstrated that pools with over 25% of aggregate processing force could get more income than decent amount. Levelheaded diggers would be pulled in into the selfish pool and finally the pool could without much of a stretch surpass 51% of the aggregate power. As the blockchain isn't planned to serve a couple of associations, a few techniques ought to be proposed to take care of this issue.

C. Big data analytics

Blockchain could be all around joined with huge information. Here we generally sorted the blend into two kinds: information administration and information examination. Concerning information administration, blockchain could be utilized to store imperative information as it is appropriated and secure. Blockchain could likewise guarantee the information is unique. For instance, if blockchain is utilized to store patients wellbeing data, the data couldn't be altered and it is difficult to stole those private data. With regards to information examination, exchanges on blockchain could be utilized for enormous information investigation. For instance, client exchanging examples may be separated. Clients can anticipate their potential accomplices' exchanging practices with the investigation.

VII.CONCLUSION

The examination demonstrates BlockChain can assume a fundamental job in changing the digitalization of ventures and applications by empowering secure trust systems and more tightly incorporation with advancements, for example, distributed computing and IOT. The Block chain is an innovation that makes it conceivable to store data without handing-off on a center man. The ends are that the Block chain is extremely helpful and pertinent in various regions where the arrangement is requesting safty, straightforwardness and adequacy. We recorded a few difficulties and future bearings are likewise proposed. Presently a day’s Block Chain based applications are jumping up and we intend to direct inside and out examination on Block Chain based applications later on. This paper exhibited how Block Chain is changing the world.

VIII. REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.
[2] S. Sargolzaei, B. Amaba, M. Abdelghani, and A. Sargolzaei, “Cloudbased Smart Health-care Platform to tackle Chronic Disease,” vol. 4863, no. August, pp. 30–32, 2016.
[3] S. Underwood, “Blockchain beyond bitcoin,” Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.
[4]G. Hurlburt, “Might the Blockchain,” no. April, pp. 12–16, 2016.

[5] B. Libert, M. Beck, and J. Wind, "How blockchain technology will disrupt financial services firms," Knowledge@Wharton, pp. 2–7, 2016.

[6] V. Buterin, "On public and private blockchains," 2015. [Online].

[7] "Hyperledger project," 2015. [Online]. Available: https://www. hyperledger.org/

[8]"Consortium chain development." [Online]. Available: https://github. com/ ethereum/ wiki/ wiki/ Consortium -Chain-Development

[9] "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends " , Zibin Zheng, Shaoan Xie, Hongning Dai,, 2017 IEEE 6th International Congress on Big Data.

[10]. S.Meiklejohn,M.Pomarole,G.Jordan,K.Levchenko,D.McCoy,G.M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA, 2013.

[11]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[12]. J. Barcelo, "User privacy in the public bitcoin blockchain," 2014.

[13]. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.

[14]. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.

[15].] K.Nayak,S.Kumar,A.Miller,andE.Shi,"Stubbornmining:Generalizing selfish mining and combining with an eclipse attack," in Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany, 2016, pp. 305–320.

[16] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," arXiv preprint arXiv:1507.06183, 2015.

[17] S. Billah, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," 2015.

[18] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin," Sorbonne Universites, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088

[19] "Crypto-currency market capitalizations," 2017. [Online]. Available: https://coinmarketcap.com

[20]."The biggest mining pools." [Online]. Available: https: //bitcoinworldwide.com/mining/pools/

[21]. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.

[17] Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[20] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[21] G. Engaged, J. Tobe, G. Your, C. Computing, C. Dellorso, E. Apps, E. Reggie, R. Coughlan, and M. S. Fernandes, "Annual Conference – May 6-7 , 2013 – Kingsmill Resort ' The Value of Values : Linking Strategy and Decision Making ' – 2013 Annual Conference Educational Sessions," 2013.

[22] W. E. Summary and S. Plants, "Power and the Industrial Internet of Things (IIoT)," no. January, pp. 1–14, 2015.

[23] U. S. D. of H. and H. Services, "Standards for privacy of individually identifiable health information; proposed rule.," Fed. Regist., vol. 64, no. 212, p. 59917, 1999.

[24] Centers for Medicare and Medicaid Services, “Security Standards: Technical Safeguards,” HIPAA Secur. Ser., vol. 2, pp. 1–17, 2007. [10] M. Modahl, “Tablets set to change medical practice,” Quantia MD, 2011.

[25]. Dr Taghreed Justinia, Introduction to blockchain and why it will transform healthcare, Blockchain in Healthcare, 2018 summit.

[26]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? A Systematic Review. PLOS ONE, 11(10), e0163477.

[27]. Lindman, J., Rossi, M., & Tuunainen, V. (2017). Opportunities and risks of Blockchain Technologies in payments – a research agenda.

[28]. White paper on “Applications of Blockchain Technology to Banking and Financial Sector in India” by IDRBT, January 2017

[29]. G. Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger – Homestead Revision. Jan. 2016. [7]. EU. (2016). Blockchain applications & services. Case study.

[30]. A. Kiayias, I. Konstantinou, A. Russell, B. David, R. Oliynykov. : Ouroboros: A provably secure proof-of-stake blockchain protocol.